

200-201^{Q&As}

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/200-201.html

100% Passing Guarantee 100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers



https://www.pass2lead.com/200-201.html

QUESTION 1

Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between tw	o IF
phones?	

- A. known-plaintext
- B. replay
- C. dictionary
- D. man-in-the-middle

Correct Answer: D

QUESTION 2

At a company party a guest asks questions about the company\\'s user account format and password complexity. How is this type of conversation classified?

- A. Phishing attack
- B. Password Revelation Strategy
- C. Piggybacking
- D. Social Engineering

Correct Answer: D

QUESTION 3

An engineer is working with the compliance teams to identify the data passing through the network. During analysis, the engineer informs the compliance team that external penmeter data flows contain records, writings, and artwork Internal segregated network flows contain the customer choices by gender, addresses, and product preferences by age. The engineer must identify protected data. Which two types of data must be identified\\'? (Choose two.)

- A. SOX
- B. PII
- C. PHI
- D. PCI
- E. copyright

Correct Answer: BC

https://www.pass2lead.com/200-201.html

2024 Latest pass2lead 200-201 PDF and VCE dumps Download

QUESTION 4

An analys	t discovers tha	t a legitimate	security ale	rt has been	dismissed.	Which:	signature	caused thi	s impact o	n network
traffic?										

- A. true negative
- B. false negative
- C. false positive
- D. true positive

Correct Answer: B

A false negative occurs when the security system (usually a WAF) fails to identify a threat. It produces a "negative" outcome (meaning that no threat has been observed), even though a threat exists.

QUESTION 5

Refer to the exhibit.

alert tcp !SHOME_NET any -> SHOME_NET 80 (flags: s; msg: "Attempt to access server is made with TCP packets"; classtype:attempted-dos; sid:1000990; rev:1;)

What is the outcome of the command?

- A. TCP rule that detects TCP packets with the ACK flag in an external FTP server
- B. TCP rule that detects TCP packets with a SYN flag in the internal network
- C. TCP rule that detects TCP packets with a ACK flag in the internal network
- D. TCP rule that detects TCP packets with the SYN flag in an external FTP server

Correct Answer: B

200-201 Study Guide

200-201 Exam Questions

200-201 Braindumps